

⑬ 日本国特許庁(JP)

⑭ 特許出願公開

⑮ 公開特許公報(A)

昭61-260735

⑯ Int.Cl.⁴

識別記号

庁内整理番号

⑰ 公開 昭和61年(1986)11月18日

H 04 L 9/02
H 04 J 3/00

Z-7240-5K
C-8226-5K

審査請求 未請求 発明の数 2 (全6頁)

⑱ 発明の名称 時分割マルチプルアクセス暗号通信方式

⑲ 特 願 昭60-102017

⑳ 出 願 昭60(1985)5月14日

㉑ 発 明 者	川 崎 晃	川崎市中原区上小田中1015番地	富士通株式会社内
㉒ 発 明 者	妹 尾 雅 之	川崎市中原区上小田中1015番地	富士通株式会社内
㉓ 発 明 者	太 田 幸 一	川崎市中原区上小田中1015番地	富士通株式会社内
㉔ 出 願 人	富士通株式会社	川崎市中原区上小田中1015番地	
㉕ 代 理 人	弁理士 松岡 宏四郎		

明 細 書

1. 発明の名称

時分割マルチプルアクセス暗号通信方式

2. 特許請求の範囲

㉖ 送信局がデータ送信用のバーストに同期信号を付加して送出する時分割マルチプルアクセス通信システムにおいて、前記送信局が前記同期信号に予め定められた変更を所定回数実行することにより、前記バーストにより伝送するデータの暗号化および復号化に使用する暗号鍵に所定の更新を行う時期を受信局に通知することを特徴とする時分割マルチプルアクセス暗号通信方式。

㉗ 送信局がデータ送信用のバーストに同期信号を付加して送出する時分割マルチプルアクセス通信システムにおいて、前記送信局が前記同期信号を行う予め定められた変更の種類と、前記バーストに付加する暗号鍵を識別する情報との組合わせにより、該バーストにより伝送するデータの暗号化および復号化に使用する暗号鍵の種類を受信局に指定することを特徴とする時分割マルチプルアセ

ス暗号通信方式。

3. 発明の詳細な説明

(概要)

送信局がデータ送信用のバーストに同期信号を付加して送出する時分割マルチプルアクセス(TDMA)通信システムにおいて、送信局が同期信号の変化を用いて暗号鍵の種類、更新時期を受信局に通知することにより、使用暗号鍵に関する情報量を削減するものである。

(産業上の利用分野)

本発明は時分割マルチプルアクセス通信システムを經由して暗号通信を行う時分割マルチプルアクセス暗号通信方式に関する。

暗号通信においては、送信側で送信データを予め定められた規則(以後暗号鍵と称する)に基づき暗号化して送信し、受信側で送信側と同一の暗号鍵に基づき復号化する。暗号化および復号化の為に使用する暗号鍵を複数種類準備し、適宜変更して使用することが、暗号化データの秘匿強度を向上する為に有効である。かかる場合に、送信側

EAST AVAILABLE COPY

で使用している暗号鍵を受信側に認識させる必要がある。

この種の暗号通信を時分割マルチプルアクセス通信システムを經由して実行する場合には、送信側から受信側へ現在使用中の暗号鍵の種類を通知する情報量は、極力削減されることが望ましい。

〔従来の技術〕

第5図は時分割マルチプルアクセス衛星通信システムにおける従来の時分割マルチプルアクセス暗号通信方式の一例を示す図であり、第6図は第5図におけるデータバーストの一例を示す図である。

送信局において、地上回線から地上回線接続インタフェース1を介してバースト組立部2に送信データDSが到着すると、バースト組立部2は、送信データDSを暗号化部3に伝送する。

暗号化部3は、暗号鍵発生部4が推論する複数種類(例えばk種類)の暗号鍵の中の、現在使用する暗号鍵に基づき送信データを暗号化し、バースト組立部2に返送する。

バースト組立部2は、暗号化部3から返送される暗号化された送信データDSに、送信局識別情報ID、暗号鍵発生部5から伝送される使用中の暗号鍵に関する識別情報(以後暗号鍵識別情報KEYと称する)、或いは同期鍵発生部5が作成するバースト同期確立用の同期語UW、更に受信局でデータバーストを受信するために必要な隠送波再生部CR、ビット再生部BT、並びに誤り検出符号その他の補助部AUXを付加して第2図に示す如きデータバーストを組立て、同期制御部6およびタイムスロット割当制御部7により指定される時間領域に、変調部8および送受信装置9を經由して衛星通信回線に送出する。なお第2図におけるGTは、隣接バーストとの衝突を防止するガード時間である。

一方受信局においては、復調部10が衛星通信回線から送受信装置9を經由して到着する信号の中から、同期制御部6およびタイムスロット割当制御部7により指定された時間領域に受信したデータバーストを隠送波再生部CRおよびビット再

生部BTを用いて復調し、バースト分解部11に伝送する。

バースト分解部11は、伝送されるデータバーストを分解し、同期語UWは同期語検出部12に伝送してバースト同期を確立させ、暗号化された送信データDSおよび暗号鍵識別情報KEYは復号化部13に伝送する。

復号化部13は、暗号鍵発生部4が推論する複数種類の暗号鍵の中から、受信した暗号鍵識別情報KEYに基づき、復号化に使用すべき暗号鍵を識別し、バースト組立部2から伝送された暗号化された送信データDSを識別した暗号鍵により復号化してバースト組立部2に返送する。

バースト組立部2は、復号化部13から返送された復号化された送信データDSを、地上回線接続インタフェース1を介して地上回線に送出する。
〔発明が解決しようとする問題点〕

以上の説明から明らかな如く、従来の時分割マルチプルアクセス暗号通信方式においては、送信局は送信データDSを暗号化するために使用した暗

号鍵を、暗号鍵識別情報KEYのみにより識別してデータバーストに付加していた。従って暗号鍵識別情報KEYの情報量が増加し、データバーストの他の情報を圧迫する恐れがあった。

〔問題点を解決するための手段〕

本発明は下記の手段を講ずることにより、前記問題点を解決する。

即ち本第一の発明においては、送信局が同期語に予め定められた変更を所定回数実行することにより、バーストにより伝送するデータの暗号化および復号化に使用する暗号鍵に所定の更新を行う時期を受信局に通知する。

また本第二の発明においては、送信局が同期語に行う予め定められた変更の種類と、バーストに付加する暗号鍵を識別する情報との組合わせにより、バーストにより伝送するデータの暗号化および復号化に使用する暗号鍵の種類を受信局に指定する。

〔作用〕

即ち本第一の発明によれば、暗号鍵の更新時期

は同期語の変更により伝達される為、データバーストに付加すべき暗号鍵を識別する情報が必要となる。

また本第二の発明によれば、データバーストに付加すべき暗号鍵を識別する情報量の一部が同期語により伝達される為、暗号鍵を識別する情報の情報量が削減される。

(実施例)

以下、本発明の一実施例を図面により説明する。

第1図は本第一の発明の一実施例による時分割マルチプルアクセス暗号通信方式を示す図であり、第2図は第1図におけるデータバーストの一例を示す図であり、第3図は本第二の発明の一実施例による時分割マルチプルアクセス暗号通信方式を示す図であり、第4図は第3図におけるデータバーストの一例を示す図である。なお、全図を通じて同一符号は同一対象物を示す。

第1図においては、送信局が暗号化に使用する暗号鍵、および受信局が復号化に使用する鍵は、暗号鍵発生部4が予め準備する m 種類の暗号鍵を、

予め定められた順序で交換して使用するものとし、送信局および受信局において当初使用する暗号鍵は、予め一致されているものとする。また同期語発生部5は複数種類(例えば m 種類)の同期語 UW を準備している。

また第2図においては、暗号鍵識別情報 KEY がデータバーストから除去されている。

送信局においては、バースト組立部2が、地上回線から地上回線接続インタフェース1を介して伝達される送信データ DS を暗号化部3により暗号化し、同期語発生部5が準備する同期語 UW の中の所定の一個を選び、搬送波再生部 CR 、ビット再生部 BT 、送信局識別情報 ID 、並びに誤り検出符号その他の補助部 AUX と共に、第4図に示す如きデータバーストを組立て、変調部8および送受信装置9を介して衛星通信回線に送信する。

送信局が現在使用中の暗号鍵を次の暗号鍵に更新する場合には、同期語 UW の種類を予め定められた回数(例えば1回)変更して送信する。

一方受信局においては、バースト分解部11が、

7

復調部10から伝達されるデータバーストを分解し、同期語 UW は同期語検出部12に伝達してバースト同期を確立させ、暗号化された送信データ DS は復号化部13に伝達する。なお同期語検出部12は、検出した同期語 UW の種類を暗号鍵発生部4および復号化部13にも伝達する。

復号化部13は、当初予め定められた暗号鍵を用いて、バースト組立部2から伝達された暗号化された送信データ DS を識別した暗号鍵により復号化してバースト組立部2に返送する。

なお同期語検出部12が伝達された同期語 UW が変更されたことを識別すると、その旨暗号鍵発生部4および復号化部13に通知する。暗号鍵発生部4は変更回数が予め定められた回数(例えば1回)に達すると、夫迄使用していた暗号鍵を次の暗号鍵に更新し、暗号化部3および復号化部13に伝達する。以後復号化部13は、新たに変更された暗号鍵を用いて、バースト分解部11から伝達される暗号化された送信データ DS を復号化する。

8

従って送信局から衛星通信回線に送信されるデータバーストには、暗号鍵識別情報 KEY を付加する必要がなくなる。

次に第3図においても、同期語発生部5は複数種類(例えば m 種類)の同期語 UW を準備している。

送信局においては、バースト組立部2が、地上回線から地上回線接続インタフェース1に到着する送信データ DS を暗号化部3により暗号化し、同期語発生部5が準備する同期語 UW の中の所定の一個を選び、暗号鍵発生部4から伝達される暗号鍵識別情報 KEY 、搬送波再生部 CR 、ビット再生部 BT 、送信局識別情報 ID 、並びに誤り検出符号その他の補助部 AUX と共に、第4図に示す如きデータバーストを組立てる。

なお暗号鍵の識別は、暗号鍵識別情報 KEY および同期語 UW の組合わせで識別させる為、暗号鍵識別情報 KEY の種類は、第5図および第6図の場合に比し $1/m$ に減少する。従ってデータバーストに付加すべき暗号鍵識別情報 KEY の所要

情報量(ビット数)も第2図に示す如く減少する。

一方受信局においては、バースト分解部11が、復調部10から伝達されるデータバーストを分解し、同期語UWは同期語検出部12に伝達してバースト同期を確立させ、暗号化された送信データDSおよび暗号鍵識別情報KEYを復号化部13に伝達する。なお同期語検出部12は、検出した同期語UWを復号化部13にも伝達する。

復号化部13は、暗号鍵識別情報KEYと、同期語検出部12から伝達される同期語UWとの組合わせに基づき、暗号鍵発生部5が準備する複数種類(1種類)の暗号鍵の中から、復号化に使用すべき暗号鍵を識別し、バースト組立部2から伝達された暗号化された送信データDSを識別した暗号鍵により復号化してバースト組立部2に返送する。

なお、第1図乃至第4図はあく正本発明の一実施例に過ぎず、例えばデータバーストの構成は図示されるものに限定されることは無く、他に幾多の変形が考慮されるが、何れの場合にも本発明の

効果は変わらない。また送信局および受信局の構成は図示されるものに限定されることは無く、他に幾多の変形が考慮されるが、何れの場合にも本発明の効果は変わらない。更に本発明の対象となる時分割マルチプルアクセス通信システムは、衛星通信システムに限定されぬことは言うまでも無い。

〔発明の効果〕

以上本発明によれば、前記時分割マルチプルアクセス通信システムにおいて、本第一の発明によれば、データバーストに付加すべき暗号鍵を識別する情報が不要となり、また本第二の発明によれば、データバーストに付加すべき暗号鍵を識別する情報量が削減され、データバースト内の他の情報量を圧迫する恐れが解消される。

4. 図面の簡単な説明

第1図は本第一の発明の一実施例による時分割マルチプルアクセス暗号通信方式を示す図、第2図は第1図におけるデータバーストの一例を示す図、第3図は本第二の発明の一実施例による時分割マルチプルアクセス暗号通信方式を示す図、第

11

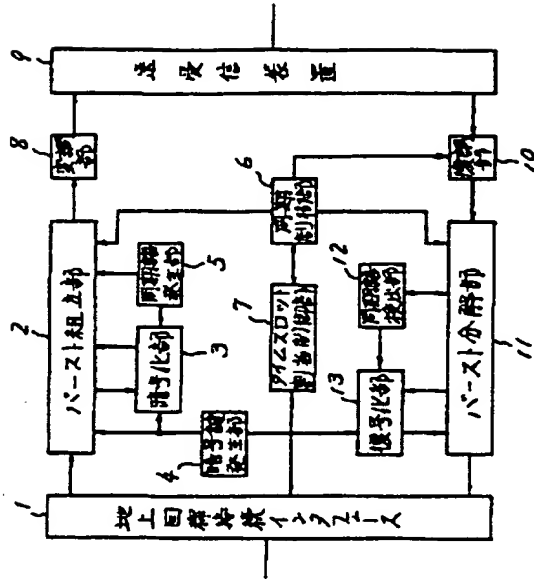
12

4図は第3図におけるデータバーストの一例を示す図、第5図は従来ある時分割マルチプルアクセス暗号通信方式の一例を示す図、第6図は第5図におけるデータバーストの一例を示す図である。

図において、1は地上回線接続インタフェース、2はバースト組立部、3は暗号化部、4は暗号鍵発生部、5は同期語発生部、6は同期語制御部、7はタイムスロット割当制御部、8は変調部、9は送受信装置、10は復調部、11はバースト分解部、12は同期語検出部、13は復号化部、AUは補助部、BTはビット再生部、CRは搬送波再生部、DSは送信データ、GTはガード時間、IDは送信局識別情報、KEYは暗号鍵識別情報、UWは同期語、を示す。

代理人 弁理士 松岡定四郎





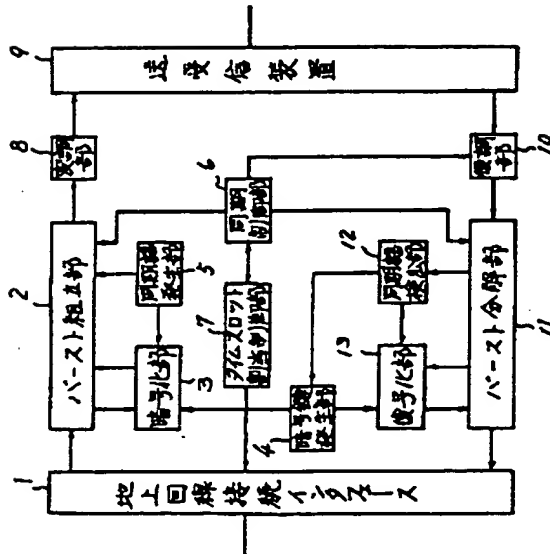
本第二の発明の実施例を示す図

第 3 図

GT CR BT UNW ID DS AUX GT

本第二の発明のデジタルベースステーションを示す図

第 4 図



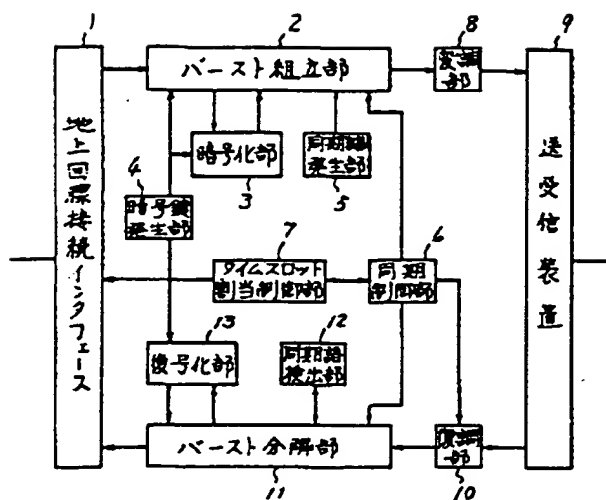
本第一の発明の実施例を示す図

第 1 図

GT CR BT UNW ID DS AUX GT

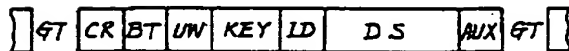
本第一の発明のデジタルベースステーションを示す図

第 2 図



従来例を示す図

第 5 図



従来あるデータパースト例を示す図

第 6 図

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINE(S) OR MARK(S) ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.